EXTENSION OF THE SIEVE OF ERATOSTHENES TO ARITHMETICAL PROGRESSIONS AND APPLICATIONS*

BY J. C. MOREHEAD

ALMOST without exception the methods employed in the elaboration of the various existing factor-tables are modifications, more or less remote, of the classic Sieve of Eratosthenes. In most instances these factor-tables are designed to show the prime numbers and the prime factors of the composite numbers occurring in sets of consecutive integers.† The Sieve method, as applied to the determination of the primes in a set of consecutive integers

$$m, \quad m+1, \quad m+2, \quad m+3, \cdots m+n,$$

may be briefly described as follows: We strike out from the numbers of the set the multiples of 2; from the remaining numbers of the set the multiples of 3; then, from those yet remaining, the multiples of 5, and so continue, for the multiples of all primes not greater than $\sqrt{(m+n)}$. The numbers finally remaining in the set are all prime. If, as the procedure just described is carried out, the multiples of 2, 3, 5, $\cdots$ are conveniently indicated, we obtain what is called a *factor-table* for the set of numbers considered.

The present paper describes an analogous method applied to successive numbers in arithmetical progression. The discussion in §§1–5 is quite general, while the remaining part of the paper is occupied with the discussion of applications and special cases.

1. Extension of the Sieve method. Any arithmetical progression of m integral terms may be written, in direct or inverse order, in either of the forms

$$(1) \qquad a^k+b, \quad 2a^k+b, \quad 3a^k+b, \cdots \quad ma^k+b,$$

$$(1') \qquad -a^k+b, \quad -2a^k+b, \quad -3a^k+b, \cdots -ma^k+b,$$

* Read before the American Mathematical Society, April 29, 1905; December 29, 1905.

† The Factor-Tables of J. Burckhardt, Z. Dase and J. Glaisher applying to all integers under 9000000, their recent extension by L. D. Lehmer, under the auspices of the Carnegie Institution, Washington, D. C., to 10000000, and the tables of "High Primes" of A. Cunningham and H. J. Woodall are the principal tables of the sort that have been satisfactorily verified.

if suitable integral values are assigned to the symbols, a, b, k, m. The following general discussion may be limited, therefore, to progressions of the forms (1) and (1′). Evidently we may assume, without loss of generality, that a is positive and k positive or zero. We shall further assume, unless the contrary is expressly stated, that b is prime to a^k;* for each term in (1) and (1′) would admit the common divisor of b and a^k as a factor, — a case which it is useless to include in a search for prime numbers or in the formation of a factor-table.

The methods and results obtained in this paper have for basis and starting point the following

THEOREM. *Let p be any prime number that does not divide a^k, and let the least non-negative solution of the congruence*

$$xa^k + b \equiv 0 \bmod p,$$

for assigned values of a, b and k, be

$$x = x_{kp}.$$

Then only the

$$(x_{kp})^{\text{th}}, \quad (p + x_{kp})^{\text{th}}, \quad (2p + x_{kp})^{\text{th}}, \cdots (pm_p + x_{kp})^{\text{th}}$$

numbers in (1) *are divisible by p and only the*

$$(p - x_{kp})^{\text{th}}, \quad (2p - x_{kp})^{\text{th}}, \quad (3p - x_{kp})^{\text{th}}, \cdots (pm'_p - x_{kp})^{\text{th}}$$

numbers in (1′) *are divisible by p, m_p and m'_p being the maximum integers such that*

$$pm_p + x_{kp}, \quad pm'_p - x_{kp} \leqq m.\dagger$$

As here defined, x_{kp} is clearly a function of k, p, a and b. This will occasionally be indicated by writing x_{kpab}. However, when it is believed that no ambiguity or confusion will arise the symbol will always be abbreviated to x_{kp} or even x_k.

The above theorem leads at once to the following

* An exception is made in the application of the relation (M) in §11.

† From well known properties of linear congruences it follows that no solution x_{kp} exists when p is a factor of a^k; but for all other prime values of p an unique solution exists such that $0 \leqq x_{kp} \leqq p - 1$, and that all other solutions are represented by

$$x = np + x_{kp},\ n = \pm 1, \pm 2, \pm 3, \cdots.$$

The validity of the theorem is thus immediately rendered apparent.

Extension of the Sieve of Eratosthenes. *Let π be the greatest prime not greater than $\sqrt{M}$, where M is the maximum numerical value of the numbers in* (1) *and* (1′) *for an assigned set of values of a, b, k and m. Let the values of x_{kp} be known for all prime values of p as far as π. Then to determine the primes in* (1) *we strike out from* (1) *the*

$$(x_{k2})^{\text{th}},\quad (2 + x_{k2})^{\text{th}},\quad (2 \times 2 + x_{k2})^{\text{th}},\quad (3 \times 2 + x_{k2})^{\text{th}}, \cdots (2m_2 + x_{k2})^{\text{th}}$$

numbers, which are multiples of 2 ; *then the*

$$(x_{k3})^{\text{th}},\quad (3 + x_{k3})^{\text{th}},\quad (2 \times 3 + x_{k3})^{\text{th}},\quad (3 \times 3 + x_{k3})^{\text{th}}, \cdots (3m_3 + x_{k3})^{\text{th}}$$

numbers, which are multiples of 3 ; *then the*

$$(x_{k5})^{\text{th}},\quad (5 + x_{k5})^{\text{th}},\quad (2 \times 5 + x_{k5})^{\text{th}},\quad (3 \times 5 + x_{k5})^{\text{th}}, \cdots (5m_5 + x_{k5})^{\text{th}}$$

numbers, which are divisible by 5 ; *and so continue, until finally we strike out from the remaining numbers the*

$$(x_{k\pi})^{\text{th}},\quad (\pi + x_{k\pi})^{\text{th}},\quad (2\pi + x_{k\pi})^{\text{th}},\quad (3\pi + x_{k\pi})^{\text{th}}, \cdots (\pi m_\pi + x_{k\pi})^{\text{th}}$$

numbers, which are multiples of π ; the numbers now remaining are the primes occurring in (1).

Similarly, to determine the primes in (1′), *we strike out from* (1′) *the*

$$\begin{array}{llll}
(2 - x_{k2})^{\text{th}}, & (2 \times 2 - x_{k2})^{\text{th}}, & (3 \times 2 - x_{k2})^{\text{th}}, \cdots & (2m_2 - x_{k2})^{\text{th}} \\
(3 - x_{k3})^{\text{th}}, & (2 \times 3 - x_{k3})^{\text{th}}, & (3 \times 3 - x_{k3})^{\text{th}}, \cdots & (3m_3 - x_{k3})^{\text{th}} \\
\cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot \\
(\pi - x_{k\pi})^{\text{th}}, & (2\pi - x_{k\pi})^{\text{th}}, & (3\pi - x_{k\pi})^{\text{th}} \cdots & (\pi m_\pi - x_{k\pi})^{\text{th}}
\end{array}$$

numbers, and those finally remaining in (1′) *are prime.*

If, as this process is carried out, the multiples of 2, 3, 5, 7, $\cdots$ π *are indicated, we obtain a factor-table for the progressions* (1) *and* (1′).

When x_{k2}, x_{k3}, x_{k5}, $\cdots$ $x_{k\pi}$ are known, this "sifting" is essentially identical with the ordinary Sieve. In order, therefore, to render this extension of the Sieve method in any degree practicable, it is necessary to devise means of calculating expeditiously the numbers x_{kp} for successive primes and for assigned values of a, b and k.

2. The calculation of x_{kp}. Connection with residue tables.

The choice of the most convenient means of computing x_{kp}, *i. e.*, of solving the congruence

$$(A) \qquad xa^k + b \equiv 0 \bmod p,$$

depends, in general, on the relative values of k, a and p. The direct solution of (A), even for small p and for the few cases where residue tables are available giving the least remainders (mod p) of a^k, is quite tedious. However, when such tables are at hand, we express the solution of(A) in the form

$$(B) \qquad x_{kp} \equiv -\frac{b}{a^k} \equiv -ba^{\nu-k} \equiv -ba^{\nu-k'} \bmod p,$$

where ν is the principal exponent* of a (mod p), and k' is the least positive remainder of k (mod ν), take the least remainder, R, of $a^{\nu-k'}$ from the tables, and compute directly x_{kp} as the least positive remainder (mod p) of $-bR$. When $b = \pm 1$, we may thus read the successive values of x_{kp} directly from the residue tables.† Thus for $a = 6$, $b = -1$, $p = 13$, $k = 8$, we have $x_8 \equiv 6^{12-8} \equiv 7 \bmod 13$.

3. Calculation of x_{k+1} from x_k. First method. In many cases, especially when series for different values of k, but fixed values of a and b, are under investigation, it is found expedient to employ one of the following methods of deriving $x_{k+1,p}$ from $x_{k,p}$, $x_{k+2,p}$, from $x_{k+1,p}$, and so on, beginning with a known x_{kp}. Setting $k = 0$ in (B), we obtain

$$(C) \qquad x_{0p} \equiv -b \bmod p.$$

Hence x_{0p} is in every case known or readily determined, and therefore the calculation of x_k for successive values of k may be begun with x_0.

Replacing x by x_k, and writing (A) in the form

$$\frac{x_k}{a} a^{k+1} + b \equiv 0 \bmod p,$$

we have at once

$$(D) \qquad x_{k+1} \equiv \frac{x_k}{a} \equiv \frac{x_k + yp}{a} \bmod p,$$

* The minimum integer, ν, such that $a^\nu \equiv 1 \bmod p$.

† The only printed residue table of sufficient extent to be of use in this connection is *A Binary Canon*, by Lt.-Col. A. Cunningham. This table gives the least positive remainders of 2^x for $x = 1, 2, 3, \cdots \nu$, and for all primes under 1000. An extension of the table (as yet in MS.), by Col. Cunningham and Mr. H. J. Woodall, includes all primes under 10000 for $x \leqq 100$, and all primes under 12000 for $x \leqq 36$. Hence when $a = 2$, $p < 12000$, and k is such that $\nu - k'$ falls within the range of values of x just stated, the *Binary Canon* is directly applicable to the computation of x_{kp}.

where y is an arbitrary integer. Since a and p are mutually prime, an unique choice of y from the numbers $0, 1, 2, \cdots a-1$ is possible, such that $(x_k + yp)/a$ is integral and less than p. When y is so chosen,* we may write instead of (D)

$$(E) \qquad x_{k+1} = \frac{x_k + yp}{a}.$$

For example, when $a = 2$, $y = 0$ or 1 according as x_k is even or odd; and therefore the computation of x_{k+1} from x_k involves simply division by 2 when x_k is even, or the addition of p and then division by 2 when x_k is odd. Thus, for $a = 2$, $b = 1$ and $p = 37$, $x_0 = 36$; $x_1 = 36/2 = 18$; $x_2 = 9$; $x_3 = (9 + 37)/2 = 23$; $x_4 = (23 + 37)/2 = 30$; etc.

Again, when $a = 10$, y may be chosen at sight so that the final digit of $yp + x_k$ will be zero.† Thus, for $a = 10$, $b = 3$, and $p = 43$, we have $x_0 = 40$; $x_1 = 4$; $x_2 = (4 + 2 \times 43)/10 = 9$; $x_3 = (9 + 7 \times 43)/10 = 31$; etc.

4. Calculation of x_{k+1} from x_k. Second method. For brevity, set $\xi_k = x_{kpa1}$ and $\xi'_k = x_{kpa'-1}$. The following relations are always satisfied, ξ_k, ξ'_k and x_k referring to the same a and p.

$$\left.\begin{array}{ll}
(F) & x_{k+1} \equiv -\xi_1 x_k \\
(F') & x_{k+1} \equiv \xi'_1 x_k \\
(G) & x_{k+h} \equiv (-\xi_1)^h x_k \\
(G') & x_{k+h} \equiv \xi'^h_1 x_k \\
(H) & x_{k+h} \equiv -\xi_h x_k \\
(H') & x_{k+h} \equiv \xi'_h x_k \\
(J) & x_{k+nh} \equiv (-\xi_h)^n x_k \\
(J') & x_{k+nh} \equiv \xi'^n_h x_k
\end{array}\right\} \bmod p.$$

* The selection of y involves the solution of the congruence $yp + x_k \equiv 0 \bmod a$, the difficulty of which, compared with the labor of solving (A) directly, will generally depend on the relative values of a, p and k. The application of $(E$, is essentially the same for k small or large, which is not the case with the solution of (A). Also, if $p > a$, the application of (E) is clearly the preferable method.

† In the case $a = 10$ the use of ordinary commercial *adding machines* greatly facilitates the de ivation of x_{k+1} from x_k; for the process reduces to the addition of p to x_k repeated until the final digit of the sum is zero, and then dropping the cipher. This procedure may be modified so as to be applicable to certain other special cases.

Evidently (F), (G) and (H) are contained in (J), and (F'), (G') and (H') are contained in (J'). All, however, are useful in computation, and are written together for convenient reference.

The demonstration of (J) and (J') establishes the validity of the six preceding relations as well. From the definitions of x_k and ξ_h we have

$$(c) \qquad x_k \equiv -ba^{-k} \bmod p,$$

$$(\gamma) \qquad -\xi_h \equiv a^{-h} \bmod p.$$

Multiplying (c) by (γ) n times, member for member, we obtain

$$(-\xi_h)^n x_k \equiv -ba^{-(k+nh)} \bmod p.$$

But by definition

$$x_{k+nh} \equiv -ba^{-(k+nh)} \bmod p;$$

therefore

$$x_{k+nh} \equiv (-\xi_h)^n x_k \bmod p.$$

The demonstration of (J') is similar.

The computation of x_{k+1}, x_{k+h}, or x_{k+nh} from x_k by means of the above relations involves only the *direct* calculation of the least positive remainder (mod p) of a product. Thus, for $p=41$, $a=14$ and $b=5$, we have, from (C) and (E),

$$\xi'_0 = 1, \quad \xi'_1 = (1+41)/14 = 3; \quad x_0 = 36,$$

and therefore, by (F'),

$$\left.\begin{array}{l} x_1 \equiv 3 \times 36 \equiv 26 \\ x_2 \equiv 3 \times 26 \equiv 37 \\ x_3 \equiv 3 \times 37 \equiv 29 \\ x_4 \equiv 3 \times 29 \equiv 5 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \end{array}\right\} \bmod 41.$$

Thus (F) and (F') are admirably adapted to the compution of x_k for successive values of k, yielding a method generally practicable. For a few special values of a, however, the method of §3 involves less reckoning and is therefore preferable. Any one of the formulas (G), (G'), $\cdots$ (J') may be employed in calculating x_k for non-consecutive values of k, — in practice, that one is selected with which the smallest ξ or ξ' may be used. Applied in this way at intervals, the congruences (G), (G'), $\cdots$ (J') are especially valuable as check formulas.

5. Relation between x_{kpab} and x_{kpa-b}. For brevity, we write $x_k = x_{kpab}$ and $x'_k = x_{kpa-b}$. By definition

$$x_k a^k + b \equiv 0 \bmod p,$$

$$x'_k a^k - b \equiv 0 \bmod p.$$

By addition, we obtain

$$(x_k + x'_k)\, a^k \equiv 0 \bmod p\,;$$

hence

$$x_k + x'_k \equiv 0 \bmod p,$$

and since x_k, $x'_k < p$, we have at once

$$(K) \qquad x_k + x'_k = p,$$

except when $x_k = x'_k = 0$, *i. e.*, when b is divisible by p. This exceptional case, b divisible by p, requires no computation, and may therefore be excluded from discussion in this and the following section.*

If b is replaced by $-b$, formula (C) becomes

$$(C') \qquad x'_{0p} \equiv b \bmod p,$$

which could have been inferred also from (K). It follows as an immediate consequence of the definition of x'_k, that the same methods and rules that apply to the computation of x_k apply equally well to the computation of x'_k, starting from the initial value given by (C').

When one of the numbers x_k, x'_k is known, the other may be obtained by the relation (K); however, when a table of successive values of x_k and x'_k together is being formed, as illustrated in §6, (K) is employed most effectively as a check formula.

6. Calculation of x_k and x'_k when $a = 2$. As has been noted in §4, the calculation of x_{k+1} from x_k by means of formula (E) is extremely simple when $a = 2$, involving only division by 2 when x_k is even, and the

* The relation (K) is contained implicitly in the theorem of §1, as may easily be seen if we note that the numbers in the series (1) and (1′), with the signs changed throughout, refer to $-b$. In fact, the x_k for the numbers in (1′), with the opposite signs, is simply $p - x_k$, *i. e.*, x'_k.

addition of p and division by 2 when x_k is odd. Even greater simplicity is attained when the computation of successive values of x_k and x'_k is performed simultaneously by a method based on the relations :*

$$x_k + x'_{k+1} = x_{k+1}, \text{ when } x_k \text{ is odd,} \tag{L}$$

$$x'_k + x_{k+1} = x'_{k+1}, \text{ when } x'_k \text{ is odd.} \tag{L'}$$

We shall demonstrate only (L), as the demonstrations of (L) and (L') are similar in form.

By definition of x_k, we have

$$x_k a^k + b \equiv 0 \bmod p,$$

and multiplying by 2,

$$x_k a^{k+1} + 2b \equiv 0 \bmod p. \tag{k}$$

Also, by definition of x'_{k+1},

$$x'_{k+1} a^{k+1} - b \equiv 0 \bmod p. \tag{k'}$$

Adding (k) and (k'), we obtain

$$(x_k + x'_{k+1}) a^{k+1} + b \equiv 0 \bmod p,$$

and therefore

$$x_k + x'_{k+1} \equiv x_{k+1} \bmod p. \tag{l}$$

In keeping with the conventions stated in §1, $p = 2$ is excluded when $a = 2$, and hence it follows from (K) that one of the numbers x_k, x'_k is even and the other odd. Let x_k be odd ; then x'_k is even and $x'_{k+1} = (x'_k)/2$. But, from (K), $x_k + x'_k = p$, and hence $x_k + x'_{k+1} = x_k + (x'_k)/2 < p$. We may therefore, when x_k is odd, replace the congruence (l) by the equation

$$x_k + x'_{k+1} = x_{k+1}.$$

The formulas (L), (L') and (E) yield the following compact method for the calculation of successive values of x_k and x'_k when $a = 2$.

* (L) and (L') are valid only for $a = 2$. The generalizations take the forms

$$x_k + (a-1)x'_{k+1} \equiv x_{k+1} \bmod p, \tag{m}$$

$$x'_k + (a-1)x_{k+1} \equiv x'_{k+1} \bmod p, \tag{m'}$$

respectively. These congruences are not especially useful in computation when $a > 2$, since when one of the numbers x_{k+1}, x'_{k+1} is known, the other can be found from (K) more readily than from (m) or (m').

The numbers x_0 and x'_0 are known and one is even; hence one of the numbers x_1, x'_1 can be obtained by a single direct division by 2, and the other by the application of (L) or (L'), involving the addition of two numbers, each of which is less than p; then one of the numbers x_2, x'_2 can be obtained by a single direct division by 2, and the other by the application of (L) or (L'); and so on, for x_3, x'_3; x_4, x'_4; $\cdots$.

The compactness of the method and the speed it is possible to attain in the reckoning are perhaps best understood in connection with a few examples arranged in tabular form as follows. The number heading each column represents k, and the upper and lower numbers of the pairs in the columns represent the corresponding values of x_k and x'_k respectively.

$k =$	0	1	2	3	4	5	6	7	8	9	10
$p = 67$ $x_k =$	60	30	15	41	54	27	47	57	62	31	49
$b = 7$ $x'_k =$	7	37	52	26	13	40	20	10	5	36	18
$p = 16231$ $x_k =$	16104	8052	4026	2013	9122	4561	10396	5198	2599	9415	12823
$b = 127$ $x'_k =$	127	8179	12205	14218	7109	11670	5835	11033	13632	6816	3408
$p = 431$ $x_k =$	430	215	323	377	404	202	101	266	133	282	141
$b = 1$ $x'_k =$	1	216	108	54	27	229	330	165	298	149	290

In the above table, the numbers in the rows x_k or the rows x'_k that are obtained by division by 2 are sufficiently evident. As illustrations of the application of (L) and (L'), we have, for $p = 67$ and $b = 7$, $x'_1 = 7 + 30 = 37$; $x'_2 = 37 + 15 = 52$; $x_3 = 15 + 26 = 41$; $x_4 = 41 + 13 = 54$; etc. For $p = 16231$ and $b = 127$, $x_6 = 4561 + 5835 = 10396$; $x'_7 = 5835 + 5198 = 11033$; etc.

As illustrated in the above cases, we always have, when $a = 2$ and b is numerically less than p, $x_1 = (p - b)/2$ and $x'_1 = (p + b)/2$,

In the manner indicated one may, after a little practice, compute a table of the kind indicated above almost as rapidly as the numbers it contains can be written down. For the single division by 2, or else the single addition, by which each of the numbers that are to be entered in the table are obtained, may be performed mentally as the numbers are recorded. Furthermore, when x_k and x'_k are calculated by this means, the formula (K) yields an independent and effective check, and one that can be applied at a glance. When the arrangement of the table is as above, for example, the sum of the two numbers in each rectangle gives the corresponding prime. However, it is unnecessary to check each pair, x_k, x'_k, but it is sufficient to apply the test at intervals of a half score terms or more. If ordinary care is exercised, a table thus computed and checked needs no further verification.

7. A table of values of x_k and x'_k for $a = 2$.[*] The author has undertaken the elaboration of a table of values of x_k and x'_k for $a = 2$, $b = 1$, $k = 1, 2, 3, \ldots 100$, and for all primes under 100000. This table is now under way. A table of x_k alone for $k = 1, 2, \cdots 19$ and for all primes under 25000 was computed[†] by the method of §3, but the formation of the larger table for both x_k and x'_k was subsequently begun anew by the more rapid method of §6. The arrangement of the table is that shown in §6, except that the first column is headed p and contains in order the successive primes 3, 5, 7, 11, $\cdots$ and the column for $k = 0$ is omitted.

The table, when completed, will be applicable to the determination of primes and the formation of factor-tables of numbers of the forms $n2^k \pm 1$ up to 10^{10}, and to the determination of all factors under 100000 of numbers of these forms beyond 10^{10}, for $k \leqq 100$.

8. An application of the table. We pass now to the application of the table to the determination of the primes in the two arithmetical series:

$$(2) \qquad 2^{19} + 1, \quad 2(2^{19}) + 1, \quad 3(2^{19}) + 1, \cdots \quad 1211(2^{19}) + 1,$$

$$(2') \quad -2^{19} + 1, \quad -2(2^{19}) + 1, \quad -3(2^{19}) + 1, \cdots -1211(2^{19}) + 1.$$

If we include 1 with the numbers in (2) and (2'), we may write instead of the two series the single arithmetical series:

$$(2'') \quad -1211(2^{19}) + 1, \quad -1210(2^{19}) + 1, \cdots$$
$$-2^{19} + 1, \quad 1, \quad 2^{19} + 1, \quad 2(2^{19}) + 1, \cdots 1211(2^{19}) + 1.$$

Writing down in order the coefficients of 2^{19}, we obtain

$$(\mathrm{II}) \quad -1211, \quad -1210, \quad -1209, \cdots$$
$$-3, -2, -1, 0, 1, 2, 3, \cdots 1209, \quad 1210, \quad 1211.$$

[*] A paper of Mr. L. L. Dines, to be published in the April number of the ANNALS, contains a detailed discussion of the case $a = 6$ and $b = 1$, with various applications and the description of a table he has elaborated.

[†] By the author and an assistant, Miss C. Ames, in April, 1905. This table is included in the appendix of the author's thesis on "Fermat's numbers and numbers of the forms $2^kq \pm 1$" on file in the Yale University Library.

Referring to the column headed 19 in the table, we find

$$x_{19,3} = 1, \quad x_{19,5} = 3, \quad x_{19,7} = 3, \quad x_{19,11} = 9, \cdots$$

Striking out from the numbers in (II), the positive and negative multiples of 3, increased by 1, —namely, 1, 4, 7, 10, 13, $\cdots$ 1201, 1204, 1207, 1210; $-2, -5, -8, -11, -14, \cdots -1202, -1205, -1208, -1211$; then from the numbers remaining in (II) the multiples of 5, increased by 3, —namely, 3, 8, 18, $\cdots$ 1203, 1208; $-7, -22, \cdots -1207$; then from those remaining the multiples of 7, increased by 3, —namely, 17, 24, $\cdots$ 1200; -4, $-18, \cdots -1194$; and so continuing, for all primes under $\sqrt{\{1211(2^{19})+1\}}$, the numbers finally remaining in (II), except 0, are the coefficients of the prime numbers that occur in the series (2″), or, which amounts to the same, in (2) and (2′).

The author has carried out the work for this series as indicated, and has found that the following numbers in (II), and these only, correspond to primes in (2″):

1198, — 1195, — 1186, — 1164, — 1156, — 1143, — 1141, — 1134, — 1129, — 1126, — 1125, — 1123
1108, — 1104, — 1095, — 1090, — 1084, — 1083, — 1060, — 1045, — 1044, — 1039, — 1030, — 1021
- 978, — 973, — 958, ± 936, — 925, — 924, — 919, — 910, ± 894, — 888, — 885, — 883
- 868, — 853, — 850, — 828, — 804, — 801, — 793, — 778, — 759, — 754, — 748, — 745
- 735, — 733, — 730, — 726, — 705, — 700, — 696, — 685, — 664, — 663, — 654, ± 609
- 603, — 601, — 600, — 595, — 579, — 556, — 540, — 534, — 520, — 493, — 484, — 463
- 460, — 456, — 444, — 441, — 421, — 415, — 414, ± 411, — 408, — 400, — 394, — 391
± 369, — 363, — 360, — 339, ± 324, — 315, — 313, — 306, — 303, — 285, — 268, — 265
± 264, — 241, — 234, — 229, — 223, — 213, — 208, — 199, — 153, — 150, — 139, — 133
- 115, — 114, — 103, — 99, — 93, — 91, — 76, — 75, — 73, — 70, ± 69, — 61
— 51, — 36, — 34, — 1,

11, 14, 26, 27, 41, 44, 50, 54, 57, ± 69, 71, 77
131, 132, 134, 147, 156, 159, 179, 191, 194, 197, 200, 212
216, 221, 225, 230, 252, 260, ± 264, 270, 282, 296, 302, 309
312, 320, ± 324, 335, 341, 356, 365, ± 369, 380, 390, 404, ± 411
417, 419, 422, 435, 440, 447, 459, 467, 470, 476, 485, 489
492, 497, 516, 524, 551, 554, 555, 582, 585, 594, ± 609, 627
629, 630, 641, 662, 671, 686, 690, 714, 719, 720, 732, 737
740, 747, 755, 762, 771, 782, 792, 795, 809, 810, 819, 827
837, 854, 875, 876, 879, 884, ± 894, 896, 929, ± 936, 942, 945
951, 987, 989, 1001, 1014, 1019, 1031, 1049, 1059, 1077, 1089, 1094
1100, 1110, 1115, 1127, 1136, 1140, 1154, 1155, 1161, 1167, 1169, 1181
1185.

The numbers above that are marked with a double sign, as ± 936, occur in both the negative and positive coefficients. Whenever such is the case, the corresponding numbers in $(2'')$, as $\pm 936(2^{19}) + 1$, differ numerically by 2, and compose what is called a "prime pair." There are eight such pairs occurring in $(2'')$.

After the table had been made, the time occupied in applying it to the determination of the primes occurring in (2) and $(2')$ was about eight hours. This is a shorter period than would be required in multiplying out the 2422 numbers in (2) and $(2')$ and consulting factor-tables like those of Burckhardt, Dase and Glaisher, if such factor-tables were extended as far as 634912769, the largest number considered. All the numbers in (2) and $(2')$ in which the coefficient of 2^{19} is numerically greater than 19 lie beyond 10^7 and hence beyond the range of the factor-tables.

In the above case, while the numbers in $(2'')$ range in numerical value from 524287 to 634912769, the "sifting" process is applied simply to the coefficients of 2^{19}, a set of consecutive integers ranging from -1211 to $+1211$. The power of the general method of this paper is due to just this feature. After a table of x_{kp} of sufficient extent to meet the requirements of the case in hand has been computed, the sifting is applied not directly to the numbers under investigation, but to a range of smaller consecutive integers, the coefficients of a^k. Thus is obtained a method, not difficult to apply, for the determination of the primes and the factorization of the composite numbers of a given form $xa^k + b$, where the investigation of each number separately would be quite impracticable.

9. Application to the factors of Fermat's Numbers. As is well known, all factors of Fermat's Numbers,* $F_n = 2^{2^n} + 1$, must be of the form

$$Q_n = q \cdot 2^{n+2} + 1.$$

All the known factors of F_n were identified by testing the divisibility of F_n by primes of the form Q_n. The primes of the form $q.2^{19} + 1$, given in §8, were tested as possible Fermat factors† for $q = 11, 14, 26, \cdots 989$, with the result that no Fermat factors were found in addition to those already known. Hence, for $n > 16$, there are no more factors of F_n in addition to those previously known, under $1001.2^{19} + 1$, or 524812289.

* F_n is known to be prime for $n = 0, 1, 2, 3, 4$, and composite for $n = 5, 6, 7, 9, 11, 12, 18, 23, 36, 38, 73$. See *Proceedings of the London Mathematical Society*, ser. 2, vol. 1, p. 175; vol. 3, p. XXI; vol. 5, p. 237; *Messenger of Mathematics*, vol. 37, p. 65; *Bulletin of the American Mathematical Society*, vol. 11, p. 343; vol. 12, p. 449.

† *I. e.*, factors of Fermat's numbers.

By making use of the 55th and 75th columns of the table described in §7, in its present extent, it was found that neither $5 \,.\, 2^{55} + 1$ nor $5 \,.\, 2^{75} + 1$ admit factors under 2000. Subsequent tests showed that both are prime, and that $5 \,.\, 2^{75} + 1$ is a factor of F_{73}. The last result was obtained by the following method.

Setting $p = 5 \,.\, 2^{75} + 1$, we have

$$5 \,.\, 2^{75} + 1 \equiv 0 \bmod p,$$

and hence, using the notation of §4,

$$\xi_{64} = x_{64p21} = 5 \,.\, 2^{11}.$$

Then applying (H) we obtain successively

$$\begin{aligned} \xi_{2^7} &\equiv - \xi_{64}^2 \equiv - 5^2 \,.\, 2^{22} \bmod p \\ \xi_{2^8} &\equiv - 5^4 \,.\, 2^{44} \\ \xi_{2^9} &\equiv - 5^8 \,.\, 2^{88} \equiv 5^7 \,.\, 2^{13} \\ &. \quad . \quad . \quad . \quad . \quad . \\ \xi_{2^{12}} &\equiv 5^{26} \,.\, 10^{29}. \end{aligned}$$

From this stage on, the numerically least remainder (mod p) of each $\xi_{2^n}^2$ was found by direct division by p. This process showed finally $\xi_{2^{73}} = 1$, and therefore that $2^{2^{73}} + 1$ is divisible by p. Thus the identification of the Fermat factor $5.2^{73} + 1$ was effected solely by the methods of the present paper,* and less arduously, as far as $\xi_{2^{12}}$, than by the usual method of calculating successively the remainders (mod p) of $2^{2^7}, 2^{2^8}, \cdots 2^{2^{73}}$.

A more detailed report on the application of the methods of this paper to Fermat's factors will be held, for the sake of completeness, until the table of §7 is further advanced.

10. Connection with Lebon's table. Professor Lebon, in a paper published in the *Bulletin of the American Mathematical Society*, vol. 13, p. 74, describes a process for the construction of a table applicable to the factorization of the numbers in arithmetical progressions in which the common difference is the simple product of consecutive primes, $2.\ 3.\ 5. \cdots p_\lambda$, and the first term is any one of the $\phi(2.\ 3.\ 5. \cdots p_\lambda)$ numbers less than and

* This method is stated briefly in different form in *Bulletin of the American Mathematical Society*, vol. 12, p. 237.

prime to the common difference. The common difference and first term, called the *base* and *index* of the progression, are represented by B and I respectively. The system of $\phi(B)$ arithmetical progressions whese general term is $BK + I$, where K is successively equal to the positive integers starting from zero, and I is prime to B, contains all prime numbers except $2, 3, 5, \cdots p_{\lambda}$, and all composite numbers except multiples of $2, 3, 5, \cdots p_{\lambda}$. The numbers recorded in the table are the minimum values of K that render $BK + I$ divisible by each successive prime following p_{λ}.* Evidently a table so constructed is applicable to the decomposition of, or the determination of the primality of successive numbers in progressions of this special form, as far as p_{ν}^{2} (the last prime included in the table), or to the investigation of the divisibility of isolated numbers in such progressions, in a manner similar to that described in the present paper. In fact, if we take $a = B$, $b = \mathrm{I}$ and $k = 1$, the numbers x_1 occurring in my table in the first column following the primes coincide, for the primes following p_{λ}, with the minimum values of K recorded in Professor Lebon's table. If the latter table is extended to include the $\phi(B)$ values of I, the complete table is clearly applicable to *successive* integers, aside from multiples of $2, 3, \cdots p_{\lambda}^{-}$, and hence applicable to the formation of factor-tables of the usual form.

However, the method of Professor Lebon is not so easily and directly applicable as is the method of the present paper to the investigation of the divisibility of numbers of the form $ma^k + b$ when k exceeds unity. Thus the special form of the numbers $m.2^k + 1$, treated in §§8, 9, would be of no advantage if the table of Professor Lebon were to be applied.

11. Application to ranges of consecutive integers. The method of this paper may be extended so as to be applicable to a range of consecutive integers without restricting the form of the progressions as in §10. Let a and k be fixed. Then, like the Lebon progressions, the system of $\phi(a^k)$ arithmetical progressions represented by $ma^k + b$, where $m = 0, 1, 2, \cdots$ and b assumes successively the $\phi(a^k)$ positive integral values less than and prime to a^k, contains all positive integers that are prime to a. Consequently, a table of values of x_{kpab} for the primes as far as π and for the $\phi(a^k)$ values of b would suffice, like the Lebon table, for the decomposition, or the determination of the primality of all numbers prime to a as far as π^2.

* A table compiled by Professor Lebon has been published under the title *Table de caractéristiques relatives à la base* 2310 *des facteurs premiers d'un nombre inférior à* 30030, Paris, 1906.

The efficiency of such a table, as well as the amount of labor involved in the compilation, will be determined by our choice of a and k. To fix ideas, suppose it is desired to construct a table effective to 10^8. A convenient choice would be $a = 10$, $k = 4$. Then the system of $\phi(10^4)$, or 4000, progressions of 10000 terms each, whose general term is $m.10^4 + b$, contains every odd number except multiples of 5, from 1 to $10^8 - 1$. To be effective as far as 10^8, the corresponding table of values of x_{4p10b} should be calculated for 1226 primes, viz., 7, 11, 13, $\cdots$ 9973.* The following is a convenient arrangement of the table. Here x_{4p10b} stands at the intersection of the row p with the column b.

$a = 10$, $k = 4$.

$b =$	1	3	7	9	. . .	233	237	
$p = 7$	5	1	0	3	. . .	3	2	. . .
11	10	8	4	2	. . .	9	5	. . .
. .	. .	. .	. .	. .	. .	. .	. .	. .
997	432	299	33	897	. . .	956	690	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

To illustrate the method of applying the table, suppose we wish to decompose the number 26840237, $= N$, say. It is easily seen that 3 is not a factor of N. Writing $N = 2684 \times 10^4 + 237$, and referring to the column headed 237, we find

$$\begin{aligned} 2684 &\not\equiv 2 \bmod 7 \\ &\not\equiv 5 \bmod 11 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &\equiv 690 \bmod 997. \end{aligned}$$

Here 690 is the *first* remainder obtained on dividing 2684 by a prime that coincides with the corresponding x_{pb}. Hence 997 is the *least* factor of N. The remaining factor, 26921, is less than 997^2 and therefore prime. Thus we have the complete decomposition, $N = 997 \times 26921$. If for the primes as far

* It is useless to include 3, as divisibility by 3 is easily tested.

as $\sqrt{N}$ no remainder were found to coincide with the corresponding x_{pb}, then would N be prime.

The application of the table would be greatly facilitated if a residue table were available, giving the least positive remainders of each integer as far as 10^4 for the prime moduli 7, 11, · · · 9973. If the arrangement of the residue table were similar to that of the above table, then to effect the decomposition of the number 26840237, for example, we should need only to compare corresponding numbers in the columns headed 2684 and 237 in the residue and factorization tables respectively, until a coincidence is discovered at $p = 997$.

The application of the above table has one evident advantage over that of Professor Lebon, covering the same range of numbers. We recognize at sight the coefficients required to express a number in the form $m.10^4 + b$; while a division must be performed to express a number in the form $m(2 \,.\, 3. \cdots p_\lambda) + b$ preliminary to applying the Lebon table. Aside from this feature, the two tables differ little in efficiency when a residue table is available with each.

The labor of compilation is not so great as to render the task impracticable. Starting from the value of x_0 given by (C), §3, we calculate successively, for given values of b and p, x_1, x_2, x_3 and finally x_4 by the method of §3. Aided by the use of calculating machines, a computer of average speed can evaluate by this method and record about one hundred and twenty x_4's per hour, when the corresponding primes contain not more than four places. The labor may be further reduced by means of a relation which we shall now derive.

Let us write, for brevity, x_b for $x_{4_p 10b}$. We have, by definition,

$$10^4 \cdot x_b + b \equiv 0 \bmod p$$

and

$$10^4 \cdot x_{b'} + b' \equiv 0 \bmod p.$$

Whence

$$10^4(x_b + x_{b'}) + b + b' \equiv \bmod p,$$

and therefore

$$(M) \qquad x_{b+b'} \equiv x_b + x_{b'} \bmod p.$$

When the numbers in column 1 have been found by the method of §3, repeated applications of (M) will give all the remaining columns. However, the relation (M) can be used most effectively if two auxiliary columns have been calculated, viz., for $b = 2, 4$.* Since two successive values of b in the table differ by 2 or 4, the addition of x_2 or x_4 to any x_b and the subtraction of p if the sum exceeds $p - 1$ will give the corresponding x_{b+2} or x_{b+4} in the next column. Thus for $p = 997$, we have $x_2 = 864$, $x_4 = 731$; $x_9 = x_7 + x_2 = 33 + 864 = 897$; $x_{237} \equiv x_{233} + x_4 \equiv 956 + 731 \equiv 690 \bmod p$.

If a calculating machine is used, a computer can evaluate by means of (M) and record from four to five hundred x_b's per hour, for primes of four places or less. The table may be checked by applying the method of §3 to every tenth or twelfth column.† We may estimate, therefore, that a single computer would require four to five years for calculating, recording and checking the x_b's for the entire table of 4000 columns and 1226 primes.‡

The generalization of the relations developed in this paper for composite moduli, and the incidental application of the methods of deriving x_{kpab} and x'_{kpab} to the calculation of power residues are only remotely connected with the purpose of this paper and will be reserved for later publication.

NORTHWESTERN UNIVERSITY,
EVANSTON, ILL.
APRIL, 1908.

* Here b is not prime to a, so that these two columns should not be included in the table. It is easily seen that (M) is valid for $b = 2, 4$.

† It is evident from the definitions that $x_b = x_{b+p}$. Hence the numbers in any row of the table recur in exact order at intervals of $10p$ in the values of b. For primes under 1000 this property facilitates the calculation to some extent.

‡ The manuscript factor-tables of Professor Kulik, left in charge of the Vienna Academy, extend to 100330201, — a little beyond the proposed limit of the factorization table here described. However, the Kulik tables are at present almost useless on account of the many errors· they contain. See *Bulletin of the American Mathematical Society*, vol. 14, p. 106.